PATENT ABSTRACTS OF JAPAN

AD

(11)Publication number : 2004-350044
(43)Date of publication of application : 09.12.2004

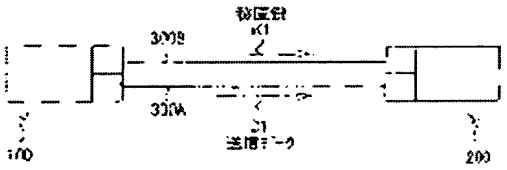
(51)Int.Cl. H04L 9/08

(21)Application number : 2003-144992
(22)Date of filing : 22.05.2003

(71)Applicant : TDK CORP
(72)Inventor : SAITO YOSHIHIRO

(54) TRANSMITTER, RECEIVER, COMMUNICATION SYSTEM, AND COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a transmitter, a receiver, a communication system, and a communication method which enhance security of communication information.
SOLUTION: A communication device 100 and a communication device 200 transmit and receive enciphered data through transmission lines 300A and 300B. Transmission data D2 is enciphered by using a secret key K1. When the transmission line 300A is used for transmission of transmission data D1, a transmission line other than the transmission line 300A< namely, the transmission line 300B is used for delivery of the secret key K1. For example, LAN cable is used as the transmission line 300A, and a power line is used as the transmission line 300B.



LEGAL STATUS

[Date of request for examination] 31.01.2006
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-350044
(P2004-350044A)
(43)公開日　平成16年12月9日(2004.12.9)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601B	5J104
	H04L	9/00	601E	

審査請求 未請求　請求項の数 19　OL　（全 21 頁）

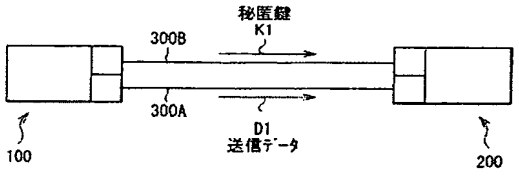
(21)出願番号　特願2003-144992(P2003-144992)
(22)出願日　平成15年5月22日(2003.5.22)

(71)出願人　000003067
ＴＤＫ株式会社
東京都中央区日本橋１丁目１３番１号
(74)代理人　100109656
弁理士　三反崎　泰司
(74)代理人　100098785
弁理士　藤島　洋一郎
(72)発明者　斉藤　義広
東京都中央区日本橋一丁目１３番１号　ティーディーケイ株式会社内

Ｆターム(参考)　5J104 EA16　EA21

(54)【発明の名称】送信機および受信機、ならびに通信システムおよび通信方法

(57)【要約】
【課題】通信情報の秘密保護を強化することが可能な送信機および受信機、ならびに通信システムおよび通信方法を提供する。
【解決手段】通信装置１００と通信装置２００は、伝送路３００Ａ，３００Ｂを介して暗号化されたデータの送受信を行う。送信データＤ１は、秘匿鍵Ｋ１を使って暗号化されている。送信データＤ１の伝送に伝送路３００Ａを用いる場合には、秘匿鍵Ｋ１の受け渡しに伝送路３００Ａ以外の経路、つまり伝送路３００Ｂを用いる。例えば、伝送路３００ＡにはＬＡＮケーブル、伝送路３００Ｂには電力線が適用される。
【選択図】　図３



【特許請求の範囲】
【請求項1】
複数の伝送路を利用して受信機との間で通信を行う送信機であって、
秘匿鍵を用いて秘匿化した送信データを、前記複数の伝送路のうちの１の伝送路を経由して前記受信機に送信すると共に、
前記秘匿鍵を、前記複数の伝送路のうちの他の伝送路を経由して前記受信機に送信する
ことを特徴とする送信機。
【請求項2】
前記秘匿鍵を送信する他の伝送路として、１つの伝送路を用いることを特徴とする請求項１に記載の送信機。
【請求項3】
前記秘匿鍵を送信する他の伝送路として、２以上の伝送路を用い、これらの伝送路に前記秘匿鍵を分割して送信する
ことを特徴とする請求項１に記載の送信機。
【請求項4】
前記送信データの種類もしくは量、前記受信機の種類、または、前記受信機が有する固有アドレス情報もしくはその固有アドレス情報の種類に応じて、前記複数の伝送路の中から前記送信データの送信に用いる伝送路と前記秘匿鍵の送信に用いる伝送路とを決定する
ことを特徴とする請求項１ないし請求項４のいずれか１項に記載の送信機。
【請求項5】
装置全体の制御を行う主制御部と、
前記複数の伝送路の各々に対応して設けられると共に、それぞれが、前記主制御部から入力された前記送信データまたは前記秘匿鍵を、対応する伝送路を経由して前記受信機に送信する複数の送信制御部と
を備え、
前記主制御部が、前記複数の伝送路の中から、前記送信データの送信に用いる伝送路と前記秘匿鍵の送信に用いる伝送路とを決定し、決定された各伝送路に対応する各送信制御部に前記送信データまたは前記秘匿鍵を渡す
ことを特徴とする請求項１ないし請求項４のいずれか１項に記載の送信機。
【請求項6】
前記複数の伝送路に対応して統括的に設けられ、前記送信データおよび前記秘匿鍵が供給される統括送信制御部を備え、
前記統括送信制御部が、前記複数の伝送路の中から、前記送信データの送信に用いる伝送路と前記秘匿鍵の送信に用いる伝送路とを決定する
ことを特徴とする請求項１ないし請求項４のいずれか１項に記載の送信機。
【請求項7】
前記送信データが複数系統の送信データを含み、
前記複数系統のうちの１の系統の送信データが送信される伝送路を経由して、他の系統の送信データの秘匿化に用いた秘匿鍵を送信する
ことを特徴とする請求項１ないし請求項６のいずれか１項に記載の送信機。
【請求項8】
前記１の伝送路と前記他の伝送路とは、互いに異なる種類の伝送路である
ことを特徴とする請求項１ないし請求項７のいずれか１項に記載の送信機。
【請求項9】
互いに異なる周波数帯の複数の搬送波を利用して受信機との間で通信を行う送信機であって、
秘匿鍵を用いて秘匿化した送信データを、前記複数の搬送波のうちの１の搬送波を用いて前記受信機に送信すると共に、
前記秘匿鍵を、前記複数の搬送波のうちの他の搬送波を用いて前記受信機に送信する
ことを特徴とする送信機。

【請求項10】
複数の伝送路を利用して送信機との間で通信を行う受信機であって、
秘匿鍵を用いて秘匿化された送信データを、前記複数の伝送路のうちの１の伝送路を経由して前記送信機から受信すると共に、
前記秘匿鍵を、前記複数の伝送路のうちの他の伝送路を経由して前記送信機から受信することを特徴とする受信機。
【請求項11】
前記秘匿鍵を受信する他の伝送路として、１つの伝送路を用いることを特徴とする請求項１０に記載の受信機。
【請求項12】
２以上の伝送路に分割されて送られてきた前記秘匿鍵を受信することを特徴とする請求項１０に記載の受信機。
【請求項13】
装置全体の制御を行う主制御部と、
前記複数の伝送路の各々に対応して設けられると共に、それぞれが、対応する伝送路を経由して前記送信機から送られてきた前記送信データまたは前記秘匿鍵を受信する複数の受信制御部と
を備え、
前記主制御部が、前記複数の受信制御部から、前記送信データおよび前記秘匿鍵を受け取る
ことを特徴とする請求項１０ないし請求項１２のいずれか１項に記載の受信機。
【請求項14】
前記複数の伝送路に対して統括的に設けられ、前記複数の伝送路を経由して送られてきた前記送信データおよび前記秘匿鍵を受信する統括受信制御部を備えた
ことを特徴とする請求項１０ないし請求項１２のいずれか１項に記載の受信機。
【請求項15】
前記送信データが複数系統の送信データを含み、
前記複数系統のうちの１の系統の送信データが送られてきた伝送路を経由して、他の系統の送信データの秘匿化に用いられた秘匿鍵を受信する
ことを特徴とする請求項１０ないし請求項１４のいずれか１項に記載の受信機。
【請求項16】
前記１の伝送路と前記他の伝送路とは、互いに異なる種類の伝送路である
ことを特徴とする請求項１０ないし請求項１５のいずれか１項に記載の受信機。
【請求項17】
互いに異なる周波数帯の複数の搬送波を利用して送信機との間で通信を行う受信機であって、
秘匿鍵を用いて秘匿化され前記複数の搬送波のうちの１の搬送波を用いて前記送信機から送信された送信データを受信すると共に、
前記複数の搬送波のうちの他の搬送波を用いて前記送信機から送信された前記秘匿鍵を受信する
ことを特徴とする受信機。
【請求項18】
複数の伝送路を利用して通信を行う通信システムであって、
秘匿鍵を用いて秘匿化した送信データを前記複数の伝送路のうちの１の伝送路を経由して前記受信機に送信すると共に、前記秘匿鍵を前記複数の伝送路のうちの他の伝送路を経由して前記受信機に送信する送信機と、
秘匿鍵を用いて秘匿化された前記送信データを前記１の伝送路を経由して受信すると共に、前記秘匿鍵を前記他の伝送路を経由して受信する受信機と
を備えたことを特徴とする通信システム。
【請求項19】

複数の伝送路を利用して送信機と受信機との間で通信を行う通信方法であって、
前記送信機は、秘匿鍵を用いて秘匿化した送信データを前記複数の伝送路のうちの１の伝送路を経由して前記受信機に送信すると共に、前記秘匿鍵を前記複数の伝送路のうちの他の伝送路を経由して前記受信機に送信し、
前記受信機は、秘匿鍵を用いて秘匿化された前記送信データを前記１の伝送路を経由して受信すると共に、前記秘匿鍵を前記他の伝送路を経由して受信する
ことを特徴とする通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、秘匿情報の伝達、特に共通鍵暗号を用いる秘匿データの通信に適用される送信機および受信機、ならびに通信システムおよび通信方法に関する。

【０００２】

【従来の技術】

通信ネットワークは、インターネットの普及等によって高速・大容量化が急速に進んでおり、一方ではユビキタスを志向した通信システムが電力線や無線などを利用して構築されつつある。こうしたネットワーク環境の発達に伴って情報の流通経路も変化し、現在では、メールやコンテンツ配信のほか、インターネットショッピング、インターネットバンキング、インターネット株取引、電子調達、電子申請、病院情報ネットワーク、企業内認証（電子社員証など）などが行われるようになっている。

【０００３】

これらの活動を、盗聴やなりすましなどが容易なインターネット上でも安全に実行できるようにするためには、セキュリティ基盤の整備が重要である。簡易なセキュリティ対策としては、データファイルにファイルを開くためのパスワードを設定すること等が広く行われており、機密情報のやりとりには、暗号化技術が用いられている。

【０００４】

例えば、共通鍵暗号方式では、送信者は、秘密にしたいデータを鍵（ある特定の変換規則）を用いて暗号化し、秘匿状態としたデータと暗号化に用いた鍵とを受信者宛てに送信する。受信者は、秘匿データと鍵を受信すると、データを鍵を用いて復号し、元の平文を得るようになっている。

【０００５】

よって、鍵がなければデータの復号は困難であることから、通信内容は第三者に対し秘匿されることになる。こうした暗号化による情報セキュリティ機能をより高める技術としては、秘匿化するデータを単独では意味のない複数のデータに分割し、それぞれを複数の通信路に振り分けて伝送するようにするものが挙げられる（特許文献１参照）。これにより、秘匿情報全体の盗聴を困難とし、たとえデータの一部が盗聴されても解読はできないようにすることが可能となる。

【０００６】

【特許文献１】

特開２０００－１１５１６２号公報

【０００７】

【発明が解決しようとする課題】

しかしながら、共通鍵暗号方式では、従来より「鍵の受け渡しかた」が問題となっていた。すなわち、盗聴などによって鍵を参照した第三者にとっては、秘匿化データを参照するのは容易であるため、いかにして通信途中で鍵を盗まれないようにするかが、データ漏洩を防止する上での焦点となっていた。

【０００８】

本発明はかかる問題点に鑑みてなされたもので、その目的は、通信情報の秘密保護を強化することが可能な送信機および受信機、ならびに通信システムおよび通信方法を提供することにある。

【０００９】
【課題を解決するための手段】
本発明の第１の観点に係る送信機は、複数の伝送路を利用して受信機との間で通信を行う送信機であって、秘匿鍵を用いて秘匿化した送信データを複数の伝送路のうちの１の伝送路を経由して受信機に送信すると共に、秘匿鍵を複数の伝送路のうちの他の伝送路を経由して受信機に送信するものである。
【００１０】
本発明における「伝送路」には、物理的な線路状媒体だけでなく、無線通信路も含まれている。物理的な線路状媒体としては、例えばイーサネット（Ｒ）などに適用されるＬＡＮケーブルや、Ｈｏｍｅ　ＰＮＡ（Ｈｏｍｅ　Ｐｈｏｎｅｌｉｎｅ　Ｎｅｔｗｏｒｋｉｎｇ　Ａｌｌｉａｎｃｅ）等で適用される電話回線、光ファイバケーブル，ケーブルテレビ（ＣＡＴＶ）のケーブル，電力線等がある。また、ここでいう無線通信路とは、有体の線路を用いずに、電波や光を用いて構成される空間伝送路をいい、例えば無線ＬＡＮ，ブルートゥース（Ｒ），ＩＲ（赤外光）通信等が含まれる。また、本発明における「秘匿鍵」には、データの内容自体を暗号化するための暗号化キーの他、データファイルの保存時に設定されるパスワードのような、データファイルを開くための単なる解除キーも含まれ、「秘匿化」するということは、送信データを秘匿鍵を用いないと解読できない状態にすることを指している。
【００１１】
本発明の第１の観点に係る送信機では、秘匿鍵が、この秘匿鍵を使って秘匿化したデータを送出する伝送路とは異なる伝送路に送出される。この送信機においては、送信データの送信に用いる伝送路と秘匿鍵の送信に用いる伝送路がともに、利用可能な複数の伝送路の中から決定される。データ送信用としては常に１の伝送路が選択されるが、秘匿鍵の送信には、例えば、この１の伝送路を除く複数の伝送路のなかから選んだ１つの伝送路だけを用いるようにしてよい。また、秘匿鍵を分割し、その分割データを２以上の伝送路の各々に送信するようにしてもよい。また、伝送路を２つとしておき、一方で送信データを伝送し、他方で秘匿鍵を伝送するようにすることもできる。
【００１２】
なお、こうした場合に、送信データおよび秘匿鍵を伝送する各伝送路は、送信データの種類もしくは量、受信機の種類、または、受信機が有する固有アドレス情報もしくはその固有アドレス情報の種類に応じて決定されることが好ましい。ここでいう「送信データの種類」とは、主としてアプリケーションソフトウェアによって定まるデータ形式を指す。例えば；ワードデータ，エクセルデータ，ＣＡＤデータ（ベクトルデータ），画像データにおけるビットマップ形式などである。「送信データの量」とは、送信データのサイズ、具体的にはファイルサイズ等である。また、「受信機の種類」とは、一般的なクライアントＰＣ（ＰＣ；パーソナルコンピュータ），サーバＰＣや、プリンタサーバ，データベースサーバ，通信サーバなど、それぞれの装置に予定されている機能や役割の種類のことをいう。さらに、「受信機が有する固有アドレス情報」とは、個々の装置を識別するために予め装置ごとに付与されている識別情報であり、例えば、ＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）で用いられるＩＰアドレスやＭＡＣアドレス（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ａｄｄｒｅｓｓ）等がある。「固有アドレス情報の種類」とは、固有アドレス情報がどのようなルールに則って（あるいは、どのような範囲で）規定されているかによる区分である。例えば、ＴＣＰ／ＩＰを例にとると、グローバルアドレスか、ローカルアドレスの区別がこれにあたる。
【００１３】
この送信機は、具体的には、装置全体の制御を行う主制御部と、複数の伝送路の各々に対応して設けられると共に、それぞれが主制御部から入力された送信データまたは秘匿鍵を対応する伝送路を経由して受信機に送信する複数の送信制御部とを備え、主制御部が、複数の伝送路の中から送信データの送信に用いる伝送路と秘匿鍵の送信に用いる伝送路とを

決定し、決定された各伝送路に対応する各送信制御部に送信データまたは秘匿鍵を渡すように構成することができる。ここでいう「主制御部」とは、送信機の各部を統括制御する部分を指す。例えば、コンピュータであれば、ＯＳが常駐すると共にこのＯＳを機能させる機能をもったメインＣＰＵを中心とした部分である。また、「送信制御部」は、例えばＮＩＣ（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）のように、伝送路と主制御部の間にあって、両者間をインタフェイス接続する部分をいう。

【００１４】

そのほか、複数の伝送路に対して統括的に設けられ、送信データおよび秘匿鍵が供給される統括送信制御部を備え、統括送信制御部が、複数の伝送路の中から、送信データの送信に用いる伝送路と秘匿鍵の送信に用いる伝送路とを決定するように構成することもできる。なお、本発明における「複数の伝送路に対して統括的に」とは、複数の伝送路のすべてに接続され、かつ、これらすべての伝送路に対応可能になっている状態を意味している。

【００１５】

さらに、送信データが複数系統の送信データを含んでいる場合には、複数系統のうちの１の系統の送信データが送信される伝送路を経由して、他の系統の送信データの秘匿化に用いた秘匿鍵を送信するようにしてもよい。この「複数系統の送信データ」とは、出所（ソース）や生成過程・処理過程等を共通として順序立てられた、統一性のある一連のデータ群が複数あることを意味している。なお、各データ群間でのデータの種類や形式の異同は問わない。

【００１６】

また、送信データの送信に用いる１の伝送路と、この送信データの秘匿化に用いられた秘匿鍵の送信に用いる他の伝送路とは、盗聴を困難にすることなどから、互いに異なる種類の伝送路であることが好ましい。

【００１７】

本発明の第２の観点に係る送信機は、互いに異なる周波数帯の複数の搬送波を利用して受信機との間で通信を行う送信機であって、秘匿鍵を用いて秘匿化した送信データを複数の搬送波のうちの１の搬送波を用いて受信機に送信すると共に、秘匿鍵を複数の搬送波のうちの他の搬送波を用いて受信機に送信するものである。なお、本発明において言う「互いに異なる周波数帯」とは、互いの周波数帯が完全に分離している場合の他、帯域の一部がオーバーラップしている場合も含んでいる。また、「搬送波を利用して」というのは、主として、搬送波によって送信データを変調することを指している。この第２の観点に係る送信機では、秘匿鍵は、（１）この秘匿鍵を使って秘匿化したデータとは、変調方式は同じだが異なった伝送帯域が用いられる場合と、（２）秘匿化したデータとは異なる変調方式に基づいて変調される場合とがある。その結果、送信データと秘匿鍵とは、互いに異なる伝送経路で伝送されることになる。

【００１８】

本発明の第１の観点に係る受信機は、本発明の第１の観点に係る送信機との間で通信を行う受信機である。すなわち、秘匿鍵を用いて秘匿化された送信データを、複数の伝送路のうちの１の伝送路を経由して送信機から受信すると共に、秘匿鍵を、複数の伝送路のうちの他の伝送路を経由して送信機から受信するものである。

【００１９】

この受信機では、利用する伝送路は送信機側と対応している必要がある。すなわち、秘匿鍵は、この秘匿鍵を使って秘匿化したデータが送られてくる伝送路とは異なる伝送路から受信される。

【００２０】

秘匿鍵の受信に用いる伝送路は、複数から選択した１の伝送路である場合や、分割された秘匿鍵の各分割データが送られてくる２以上の伝送路である場合がある。また、２つの伝送路のうち、送信データ用ではないもう一方の伝送路としてもよい。受信機の具体的構成としては、例えば、装置全体の制御を行う主制御部と、複数の伝送路の各々に対応して設けられると共に、それぞれが送信機から送られてきた送信データまたは秘匿鍵を対応する

伝送路を経由して受信する複数の受信制御部とを備え、主制御部が、複数の受信制御部から送信データおよび秘匿鍵を受け取るようにすることができる。なお、この場合の「主制御部」，「受信制御部」の定義は、上記本発明の送信機における「主制御部」，「送信制御部」の定義と同様である。

【００２１】

また、この受信機は、複数の伝送路に対応して統括的に設けられ、複数の伝送路を経由して送られてきた送信データおよび秘匿鍵を受信する統括受信制御部を備えるようにしてもよい。さらに、送信データが複数系統の送信データを含んでいる場合に、複数系統のうちの１の系統の送信データが送られてきた伝送路から、他の系統の送信データの秘匿化に用いられた秘匿鍵を受信するようにしてもよい。また、送信データが送られてくる１の伝送路と、この送信データの秘匿化に用いられた秘匿鍵を受信する他の伝送路とは、互いに異なる種類の伝送路であることが好ましい。

【００２２】

本発明の第２の観点に係る受信機は、本発明の第２の観点に係る送信機との間で通信を行う受信機であり、秘匿鍵を用いて秘匿化され、複数の搬送波のうちの１の搬送波を用いて送信機から送信された送信データを受信すると共に、複数の搬送波のうちの他の搬送波を用いて送信機から送信された秘匿鍵を受信するものである。この第２の観点に係る受信機では、秘匿鍵は、秘匿化したデータの伝送帯域とは異なる帯域において受信される。

【００２３】

本発明による通信システムは、複数の伝送路を利用して通信を行う通信システムであって、秘匿鍵を用いて秘匿化した送信データを複数の伝送路のうちの１の伝送路を経由して受信機に送信すると共に、秘匿鍵を複数の伝送路のうちの他の伝送路を経由して受信機に送信する送信機と、秘匿鍵を用いて秘匿化された送信データを１の伝送路を経由して受信すると共に、秘匿鍵を他の伝送路を経由して受信する受信機とを備えたものである。

【００２４】

本発明による通信方法は、複数の伝送路を利用して送信機と受信機との間で通信を行う通信方法であって、送信機は、秘匿鍵を用いて秘匿化した送信データを複数の伝送路のうちの１の伝送路を経由して受信機に送信すると共に、秘匿鍵を複数の伝送路のうちの他の伝送路を経由して受信機に送信し、受信機は、秘匿鍵を用いて秘匿化された送信データを１の伝送路を経由して受信すると共に、秘匿鍵を他の伝送路を経由して受信するものである。

【００２５】

本発明による通信システムおよび通信方法では、秘匿鍵と、この秘匿鍵を使って秘匿化したデータとは、互いに異なる伝送路を介して送受信される。

【００２６】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して詳細に説明する。

【００２７】

〔第１の実施の形態〕

図１は、本発明の第１の実施の形態に係る通信システムの基本構成を表している。この通信システムは、ホームネットワークを想定しており、通信装置１００と通信装置２００とが伝送路３００（３００Ａ，３００Ｂ）を介して相互に送受信を行うようになっている。伝送路３００にはＬＡＮケーブルを用いるのが一般的であるが、そのほか電話回線，ＣＡＴＶケーブル，電力線などの任意の伝送媒体を用いることができる。ここでは、最も基本的な態様として、通信装置１００と通信装置２００が、伝送路３００Ａ，３００Ｂの２本で接続されている場合について説明する。

【００２８】

ただし、このように通信網を２重に敷設するようなことは、一般家庭に限らずとも通常の使用では考えにくい。そこで、まず伝送路３００Ａを、既設あるいは新設するイーサネット（Ｒ）ケーブルとし、伝送路３００Ｂには、別の既設媒体として電力線を利用するよう

にしている。こうした線路選択は最も現実的であり、比較的簡易にシステムを構築できる。なお、イーサネット（Ｒ）に適用されるケーブルとしては、ＵＴＰケーブル（Ｕｎｓｈｉｅｌｄｅｄ　Ｔｗｉｓｔｅｄ　Ｐａｉｒ　Ｃａｂｌｅ），同軸ケーブル，光ファイバなどがある。電力線による通信システムは、既設の電力線が媒体であることから低コストであり、電気コンセントで接続できるため、ほとんどの部屋で場所を選ばず、簡便に利用できるという利点を持ち、米国では既に伝送速度１４Ｍｂｐｓで標準化されている。また、無線通信では、コンクリート構造，鉄筋構造，土壁などの建造物、さらには室内の人間や什器等によって電波が遮断され、通信状態が不安定化する傾向があるが、電力線通信は、こうした要因による通信状態の劣化が少ないと考えられる点でも有利である。

【００２９】

通信装置１００は、本体部１０と、本体部１０と伝送路３００Ａ，３００Ｂの各間にあって、それぞれの間をインタフェイス接続する通信制御部１１Ａ，１１Ｂとを備えている。通信装置２００も、本体部２０，通信制御部２１Ａ，２１Ｂを備えている。本体部１０，本体部２０は、例えばＰＣやワークステーション等であり、その場合の通信制御部１１Ａ，１１Ｂないし通信制御部２１Ａ，２１Ｂは、モデムやＮＩＣの類、すなわちデータ回線終端装置（Ｄａｔａ　Ｃｉｒｃｕｉｔ　ｔｅｒｍｉｎａｔｉｎｇ　Ｅｑｕｉｐｍｅｎｔ：ＤＣＥ）に相当する。ＮＩＣは、ＰＣ等を伝送路（一般的にはＬＡＮ）に接続するため、その拡張スロットに装着されるインターフェイス機器である。ＮＩＣには、ＩＳＡ，ＰＣＩなどの拡張バスの種類や通信方式によってイーサネット（Ｒ）・アダプタ，１００ＢＡＳＥ－Ｔ／１００ＶＧ－ＡｎｙＬＡＮアダプタ，トークンリング・アダプタ，ＦＤＤＩ（Ｆｉｂｅｒ　Ｄｉｓｔｒｉｂｕｔｅｄ　Ｄａｔａ　Ｉｎｔｅｒｆａｃｅ）アダプタなどがある。ここでは、伝送路３００Ａ（イーサネット（Ｒ）ケーブル）に接続される通信制御部１１Ａ，通信制御部２１ＡがＮＩＣ、伝送路３００Ｂ（電力線）に接続される通信制御部１１Ｂ，２１Ｂが電力線用モデムとなっている。

【００３０】

図２は、通信装置１００の構成を表している。なお、通信装置２００は、これに対応した構成となっているため、ここでは説明を省略する。

【００３１】

本体部１０は、装置全体の制御を行うメインＣＰＵ１を中心として、秘匿化部２，復号部３，メインＣＰＵ１と通信制御部１１Ａ，１１Ｂの間のデータ入出力を行うＩ／Ｏ部４Ａ，４Ｂ、さらには図示しないメモリ等を備えたものである。暗号化部２は、送信するデータを暗号化することによって、秘匿鍵を用いないと解読できない状態にするものであり、暗号化したデータおよび用いた鍵をメインＣＰＵ１に出力するようになっている。また、復号部３は、メインＣＰＵ１から暗号データと鍵を受け取って復号するようになっている。メインＣＰＵ１は、（１）暗号化部２から入力される送信用の暗号データと、その暗号化に用いた鍵とを、通信制御部１１Ａ，通信制御部１１Ｂに対して振り分けて出力する機能と、（２）受信されてくる暗号データ，暗号化に用いた鍵を、復号化部３に送出する機能を有している。

【００３２】

通信制御部１１Ａは、本体部１０－伝送路３００Ａの間のインタフェイス機能を有しており、Ｉ／Ｏ部５Ａ，ＣＰＵ６Ａ，ＲＡＭ７Ａ、およびイーサネット（Ｒ）物理層機能部（ｐｈｙｓｉｃａｌ　ｌａｙｅｒ：　ＰＨＹ）８Ａを備えている。イーサネット（Ｒ）物理層機能部８Ａは、ビットデータを符号化し、伝送媒体に適した信号形式に変換するといった通常の物理層を含み、さらに媒体へのアクセスを制御する、いわゆるＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）処理も階層的に行うようになっている。このイーサネット（Ｒ）物理層機能部８Ａには、ＬＡＮポートを介してＬＡＮケーブル（伝送路３００Ａ）が接続されている。

【００３３】

一方、通信制御部１１Ｂは、本体部１０－伝送路３００Ｂの間のインタフェイス機能を有しており、Ｉ／Ｏ部５Ｂ，ＣＰＵ６Ｂ，ＲＡＭ７Ｂ、およびＡＣ用物理層機能部８Ｂを備

えている。ここで、ＡＣ用物理層機能部８Ｂはイーサネット（Ｒ）物理層機能部８Ａに対応させて便宜的に設定したものであり、ＭＡＣ処理を行うＭＡＣ副層および物理層に対応する。この場合の物理層は、ＦＤＭ（Ｆｒｅｑｕｅｎｃｙ Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅｘ：周波数分割多重）もしくはＯＦＤＭ（Ｏｒｔｈｏｇｏｎａｌ Ｆｒｅｑｕｅｎｃｙ Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅｘ：直交周波数分割多重）などの変調方式によりシリアルビットストリームをＡＣ伝送用帯域の電気信号に変換するものである。このようなＡＣ用物理層機能部８Ｂには、コンセントを介して電力線（伝送路３００Ｂ）が接続されている。

【００３４】

なお、本明細書の以下の説明では、通信制御部がデータを本体部から伝送路へと送出する際に行う処理をまとめて変調といい、伝送路から本体部へ取り込む際に行う、変調とは逆の処理を復調ということにする。また、本実施の形態においては、通信装置１００，２００が本発明の「送信機」および「受信機」の一具体例に対応している。さらに、本体部１０，２０のメインＣＰＵが本発明の「主制御部」に、通信制御部１１Ａ，１１Ｂ、通信制御部２１Ａ，２１Ｂのそれぞれが本発明の「送信制御部」および「受信制御部」の一具体例に対応している。

【００３５】

次に、この通信システムの動作について説明する。

【００３６】

ここでは、一例として、秘匿化データを通信装置１００から通信装置２００に送信する場合について説明する。この通信システムの基本動作は、図３に示したように、暗号化された送信データＤ１を伝送路３００Ａを使って送受するとき、その秘匿鍵Ｋ１の受け渡しには、伝送路３００Ａとは異なる経路、つまり伝送路３００Ｂを用いるというものである。図４は、そうした動作の詳細を示すフローチャートであり、図５は、通信装置１００，２００の間の応答過程を示すタイミングチャートである。

【００３７】

まず、通信装置１００の本体部１０において、送信しようとするデータＤ１を暗号化部２が暗号化する。ここで用いられる暗号化方式は、例えばＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）などである。秘匿鍵Ｋ１は、繰り返し用いられるように予め定められていても構わないが、ここでは、データの暗号化の度に新たに生成されるものとする。こうして、秘匿鍵Ｋ１が生成されると共に、送信データＤ１が暗号化される（ステップＳ１）。暗号化部２は、送信データＤ１，秘匿鍵Ｋ１の双方をメインＣＰＵ１に出力する。

【００３８】

〈データの振り分け〉

メインＣＰＵ１は、入力された送信データＤ１，秘匿鍵Ｋ１を、伝送路３００Ａ，３００Ｂ（直接には通信制御部１１Ａ，１１Ｂ）に向けて振り分ける（ステップＳ２）。この振り分けかたは、システムの状況に応じていろいろなやり方を考えることができるが、例えば、伝送するデータのサイズにあわせて伝送路３００を選ぶとよい。ここでは、伝送路３００Ａのほうが伝送路３００Ｂよりも高速で伝送容量も大きいことから、送信データＤ１を伝送路３００Ａに接続された側の経路に送出し、それほどサイズが大きくならないことが想定される秘匿鍵Ｋ１を伝送路３００Ｂの側の経路に送出するようにしている。

【００３９】

メインＣＰＵ１から送出された送信データＤ１は、Ｉ／Ｏ部４Ａを介して通信制御部１１Ａに入力され（ステップＳ３）、一方の秘匿鍵Ｋ１は、Ｉ／Ｏ部４Ｂを介して通信制御部１１Ｂに入力される（ステップＳ６）。

【００４０】

〈変調〉

通信制御部１１Ａでは、送信データＤ１が、Ｉ／Ｏ部５Ａを介してＣＰＵ６Ａに入力される。ＣＰＵ６Ａは、ＲＡＭ７Ａを適宜利用しつつ通信に必要なＴＣＰ，ＩＰ等のヘッダを

送信データＤ１に付加し、さらにイーサネット（Ｒ）物理層機能部８Ａに送出する。イーサネット（Ｒ）物理層機能部８Ａは、送信データＤ１のＭＡＣフレームを生成し、さらに符号化などを経て、伝送路３００Ａ（イーサネット（Ｒ）ケーブル）に対応する形式の信号にまで変換する。このようにして、送信データＤ１は通信制御部１１Ａにて変調され（ステップＳ４）、伝送路３００Ａに送出される（ステップＳ５）。

【００４１】

一方、通信制御部１１Ｂでは、秘匿鍵Ｋ１が、通信制御部１１Ａにおける送信データＤ１と同様にして、伝送路３００Ｂ（電力線）に適応する信号形式にまで変調される（ステップＳ７）。そののち、この秘匿鍵Ｋ１は、伝送路３００Ｂに送出される（ステップＳ８）。

【００４２】

この場合、伝送路３００Ａ，３００Ｂにおけるデータ送受信の具体的状況は、例えば図５のように表される。まず、伝送路３００Ｂの上を、通信装置１００から通信装置２００へ秘匿鍵Ｋ１が送信される。通信装置２００は、秘匿鍵Ｋ１を受け取ると、伝送路３００Ｂを使って通信装置１００へ受信返答を送る。通信装置１００は、この受信返答を確認した後に、今度は伝送路３００Ａを使って通信装置２００に送信データＤ１を送出する。通信装置２００は、送信データＤ１を受け取ると、伝送路３００Ａを使って通信装置１００へ受信返答を送る。この送信データＤ１送出の過程は、例えば送信データＤ１のフレームごとに繰り返し行われる。通信装置１００は、送信データをすべて送った後、通信装置２００からの受信返答を受けると、最後に通信装置２００に対してデータ・エンド信号を送出する。

【００４３】

なお、図６は、以上の様子をデータフローブロックで表したものである（送信のみ、受信返答は省略）。伝送路３００上における送信データＤ１，秘匿鍵Ｋ１は、図示したように、前述の通信制御部１１Ａ，１１Ｂの処理によってヘッダが付加されたフレームの状態である。なお、ここでは、秘匿鍵Ｋ１を送信データＤ１よりも先に伝送するようにしているが、これら秘匿鍵Ｋ１，送信データＤ１が受信側の通信装置２００において対のデータであることが認識されるのであればよく、データの送出順はどのようであっても構わない。

【００４４】

このように、送信データＤ１と秘匿鍵Ｋ１を別々の経路で伝送するようにすると、両方がともに傍受されるおそれが減る。仮に、伝送路３００Ａにおいて送信データＤ１が漏洩したとしても、秘匿鍵Ｋ１がなければ、その解読は非常に困難である。逆に、伝送路３００Ｂが傍受されても、秘匿鍵Ｋ１だけしか参照されることはなく、送信データＤ１そのものは無事である。よって、送信データＤ１，秘匿鍵Ｋ１の両方を不正に入手するには、伝送路３００Ａ，３００Ｂの双方で傍受するしかなく、従来のように同一の線路上に送信データと鍵を伝送する場合に比べ、データ漏洩のリスクが低減される。特に、ここでは伝送路３００Ａと伝送路３００Ｂは異なる種類の線路であり、両方の傍受にはより手間がかかるようになっているため、漏洩リスク軽減のうえで好ましい。

【００４５】

次に、伝送路３００Ａに送出された送信データＤ１は、通信装置２００の通信制御部２１Ａに入力され（ステップＳ９）、伝送路３００Ｂに送出された秘匿鍵Ｋ１は通信制御部２１Ｂに入力される（ステップＳ１１）。

【００４６】

〈復調〉

送信データＤ１は、通信制御部２１Ａにて、通信制御部１１Ａで施された過程とは逆の過程を辿ることにより、復調される（ステップＳ１０）。ただし、この時点では、送信データＤ１はまだ暗号化された状態にある。一方、秘匿鍵Ｋ１もまた同様に、通信制御部２１Ｂにて復調される（ステップＳ１２）。

【００４７】

次いで、これら送信データＤ１，秘匿鍵Ｋ１は共に、本体部２０に入力され、メインＣＰ

Ｕ１を介して復号部３に入力される（ステップＳ１３）。復号部３では、秘匿鍵Ｋ１を用いて送信データＤ１が解読される（ステップＳ１４）。こうして、通信装置２００において送信データＤ１の平文が入手される。

【００４８】

なお、以上は、通信装置１００から通信装置２００へデータを送信する場合について説明したが、通信装置２００から通信装置１００へデータを送信する場合も同様に行うことができる。すなわち、両者間では、伝送路３００Ａでデータを伝送し、伝送路３００Ｂで秘匿鍵を伝送することにより送受信が行われる。

【００４９】

このように本実施の形態では、２つの伝送路３００Ａ，３００Ｂのそれぞれに、暗号化した送信データＤ１と暗号化に用いた秘匿鍵Ｋ１を別々に伝送するようにしたので、両方がともに傍受されるおそれが減り、データ漏洩のリスクを軽減することができる。

【００５０】

また、ここでは、伝送路３００Ａと伝送路３００Ｂは種類の異なる媒体であることから、双方の傍受をさらに困難としてより秘匿データの安全性を高めることができるほか、同一の媒体をわざわざ２重に敷設するという手間をかけず、適宜に使用可能な媒体を利用して構築できるという利点がある。

【００５１】

次に、上記第１の実施の形態の変形例について説明する。

【００５２】

〔変形例１〕

第１の実施の形態では、送信データは伝送路３００Ａ、秘匿鍵は伝送路３００Ｂに振り分けて伝送するようにしたが、このように伝送路３００Ａ，３００Ｂの役割を固定せず、状況に応じて送信データ，秘匿鍵を伝送路３００Ａ，３００Ｂのそれぞれが割り当てられるようにすることができる。例えば、図７のように、第１の実施の形態と同様の通信システムにおいて、送信データＤ１については伝送路３００Ａに送信データＤ１、伝送路３００Ｂにその秘匿鍵Ｋ１を送出する。しかし、送信データＤ２については、逆に伝送路３００Ａに秘匿鍵Ｋ２、伝送路３００Ｂに送信データＤ２を送出する場合である。

【００５３】

図８は、第１の変形例におけるデータ通信動作のタイミングチャートである。同図の場合、まず送信データＤ１（および秘匿鍵Ｋ１）の送信を行った後、送信データＤ２（および秘匿鍵Ｋ２）の送信を行うようになっている。送信データＤ２では、送信データＤ１の送信時とは振り分け先の伝送路３００が異なるだけで、秘匿鍵Ｋ２の生成から復号までの一連の過程は同様に行われる。

【００５４】

また、図９は、この第１の変形例におけるデータフローブロックの例を示している。この場合には、図８とは異なり、送信データＤ１と送信データＤ２の送信がほぼ同時に行われている。これまでの方式では、第１の実施の形態にて前出のデータフロー（図６）からわかるように、秘匿鍵Ｋ１を伝送路３００Ｂに伝送しているときには、伝送路３００Ａは利用されていない。次いで、送信データＤ１を伝送路３００Ａに伝送しているときには、伝送路３００Ｂが空いている。そこで、この例では、送信データＤ１，Ｄ２のデータフローがモザイク状となる格好にして、２種類のデータの通信をほぼ同時に行っている。送信データおよび秘匿鍵は、振り分けられた後はあたかも互いに独立したデータのように決められた伝送路３００を伝送され、通信装置２００において送信データと秘匿鍵が対照される。

【００５５】

こうした送信データに応じた伝送路３００Ａ，３００Ｂの使い分けは、例えば、以下のようなデータ振り分け条件に基づいて行われる。

▲１▼送信データの種類。例えば、ワードデータ，エクセルデータ，ＣＡＤデータ（ベクトルデータ），ビットマップ形式の画像データなどのデータ形式に応じて、伝送路３００

Ａ，３００Ｂのいずれかに送信データを振り分け、残ったもう一方の伝送路に秘匿鍵を振り分ける。通常、ＣＡＤデータや画像データは文書に比べてサイズが大きいので、より伝送速度が大きい伝送路に優先的に送出することが考えられる。なお、インターネットのホームページなど、１つのデータファイルに画像と文章が存在する場合には、一旦、画像ファイルと文書ファイルに分割し、それぞれについて伝送路を決定することもできる。その場合、各分割データを１つの送信データとみたて、それぞれについて暗号化処理を施し、対応する秘匿鍵を生成するようにしてもよい。

【００５６】

▲２▼受信側の装置の種類。通信装置には、一般的なクライアントＰＣやサーバＰＣ、プリンタサーバ、データベースサーバ、通信サーバ等があるが、そうした装置の種類に応じてデータを振り分ける。さらには、そのうち機密性が高い装置に対してのみ、こうした２重の伝送路による通信を行うように制御するようにしてもよい。

【００５７】

▲３▼受信側の個々の装置が有する固有アドレス情報。例えばＩＰアドレスやＭＡＣアドレスを参照することにより、受信側の装置のそれぞれに対応させてデータの振り分け方を決めることができる。

【００５８】

▲４▼受信側装置のＩＰアドレスの種類。つまり、グローバルアドレスか、ローカルアドレスかを基準にして行うこともできる。この区別は、一般家庭であれば受信相手が屋外（インターネットを通じて接続）であるか、屋内（ＬＡＮで接続）であるかということになる。

【００５９】

▲５▼伝送路３００Ａ，３００Ｂの混み具合。例えば、送信前に伝送路３００Ａの混み具合を判断し、ある程度以上混んでいる場合には送信データは伝送路３００Ｂに送出するようにする。

【００６０】

〔変形例２〕

図１０は、第２の変形例に係る通信システムの構成図である。第１の実施の形態では、通信装置１００，２００は伝送路ごとに通信制御部を備えるようにしたが、本変形例では、通信装置１０１，２０１はそれぞれ１つの通信制御部１１，２１を備え、通信制御部１１，２１が伝送路３００Ａ，３００Ｂの双方に接続されている。これら通信制御部１１，２１は、単にデータを出力するためのインターフェイス機能を果たすだけではなく、送信の際には暗号化された送信データとその秘匿鍵を伝送路３００Ａ，３００Ｂのいずれに送出するかを判断する機能を有している。なお、通信装置１０１と通信装置２０１とは、対応関係にある構成要素によって対称な構成となっているものとする。

【００６１】

次に、図１１を参照して通信装置１０１の構成について説明する。本体部３０は、第１の実施の形態における本体部１０と同様の構成要素からなる（詳細は図示せず）。ただし、本体部１０のメインＣＰＵ１に与えられていた「送信データ，秘匿鍵を伝送路に振り分ける」機能は、本体部３０のメインＣＰＵにはない。よって、本体部３０は、通信制御部１１との間では暗号化した送信データおよび秘匿鍵のやり取りを行うだけである。

【００６２】

一方、通信制御部１１は、通信制御部１１Ａ，１１Ｂを統合したようになっており、伝送路３００Ａ，　３００Ｂに対して総括的に設けられている。通信制御部１１は、Ｉ／Ｏ部５，ＣＰＵ６，ＲＡＭ７，イーサネット（Ｒ）物理層機能部８ＡおよびＡＣ用物理層機能部８Ｂを備えており、ここでは、ＣＰＵ６が「送信データ，秘匿鍵を伝送路に振り分ける」機能を有している。すなわち、データ送信時には、本体部３０からＩ／Ｏ部５を通じて送信データとその秘匿鍵が入力され、ＣＰＵ６は、これらを伝送路３００Ａ，３００Ｂごとに振り分けて、それぞれイーサネット（Ｒ）物理層機能部８Ａ，ＡＣ用物理層機能部８Ｂに入力する。送信データと秘匿鍵は、イーサネット（Ｒ）物理層機能部８Ａ，ＡＣ用物

理層機能部８Ｂを介して、それぞれ伝送路３００Ａ，３００Ｂに送出される。また、この通信制御部１１は、伝送路３００Ａ，３００Ｂのそれぞれを経由して送られてくる送信データおよび秘匿鍵の両方とも受信するようになっている。

【００６３】

以上の通信装置１０１の本体部３０、通信制御部１１の作用構成は、通信装置２０１の本体部４０、通信制御部２１についても同様である。なお、この第２の変形例においては、ＣＰＵ６が本発明の「総括送信制御部」および「総括受信制御部」に対応し、通信制御部１１、２１が本発明の「送信機」および「受信機」に対応する一具体例となっている。

【００６４】

このように第２の変形例では、通信制御部１１、２１が、本体部３０、４０と伝送路３００とのインターフェイス機能に加え、「送信データと秘匿鍵の振り分け」機能を備えるようにしたので、本体部３０、４０には、旧来のＰＣ等をそのまま適用することができる。すなわち、第１の実施の形態の通信装置１００，２００では、通常用いられるＰＣカードを伝送路３００ごとに設ければよい代わりに、本体部１０、２０のメインＣＰＵ１にデータ振り分け機能を追加設定しなければならない。これに対し、本変形例では、データ振り分け機能を有し、複数の伝送路に接続可能な１枚のＰＣカードを装着するだけで済むために、システムをより簡便に構築できると考えられる。

【００６５】

〔第２の実施の形態〕

図１２は、第２の実施の形態に係る通信システムの構成を表したものである。この通信システムは、伝送路３００Ｂ（電力線）を伝送路３００Ｃ（無線）に替えたことに関したことを除けば第１の実施の形態のシステムと同様に構成されている。なお、以下の実施の形態においては、それより先に説明した実施の形態を受けて説明するものとし、同様の構成要素については同一の符号を付し、説明を適宜省略するものとする。

【００６６】

伝送路３００Ｃは、無線ＬＡＮ，ブルートゥース（Ｒ），ＩＲ（赤外光）通信などの無線通信による伝送経路である。これら無線通信では、装置の設置場所を選ばず、屋外・屋内で、また移動しながら送受信を行うことができ、物理的線路の敷設が不要なために極めて簡単に構築できる。そのため、インターネットの中継スポットとして、また、ネット家電や携帯端末を結ぶホームネットワーク等に利用されつつある。

【００６７】

この伝送路３００Ｃは、一端が通信装置１０２の通信制御部１１Ｃに接続され、他端が通信装置２０２の通信制御部２１Ｃに接続されている。通信制御部１１Ｃ，２１Ｃはともに、無線ＬＡＮカードもしくはブルートゥース（Ｒ）ＰＣカード等であり、図１３のように構成されている。これらは、Ｉ／Ｏ部５Ｃ，ＣＰＵ６Ｃ，ＲＡＭ７Ｃおよび無線用物理層機能部８Ｃを備えている。このうち、無線用物理層機能部８Ｃが、ＯＦＤＭ等の方式によって、データをそれぞれの規格に応じた電波もしくは光に変換し出力するようになっている。

【００６８】

したがって、本実施の形態における通信システムの動作は、第１の実施の形態における通信制御部１１Ｂの動作を通信制御部１１Ｃが、通信制御部２１Ｂの動作を通信制御部２１Ｃがそれぞれ行うものとすれば説明できる。また、本実施の形態におけるシステムに上記変形例の伝送手法を適用することも可能である。

【００６９】

このように本実施の形態における通信システムは、２つの伝送路３００Ａ，３００Ｃのそれぞれに暗号化した送信データと暗号化に用いた秘匿鍵を振り分けて伝送するようにしたので、第１の実施の形態と同様の効果を奏する。また、無線通信は一般に有線通信に比べてセキュリティが脆弱であることが知られているが、伝送路３００Ｃだけでなく伝送路３００Ａを利用したこの手法によって脆弱性を補完することができる。

【００７０】

〔第３の実施の形態〕
図１４は、第３の実施の形態に係る通信システムの構成を表したものである。この通信システムは、第１および第２の実施の形態の各システムを合体したようになっている。すなわち、本体部５０，通信制御部１１Ａ～１１Ｃを備えた通信装置１０３と、本体部６０，通信制御部２１Ａ～２１Ｃを備えた通信装置２０３とが、伝送路３００（３００Ａ，３００Ｂ，３００Ｃ）を介して相互に送受信を行うようになっている。通信制御部１１Ａ～１１Ｃ，２１Ａ～２１Ｃおよび伝送路３００Ａ～３００Ｃについては、第１および第２の実施の形態で説明した通りである。ただし、この場合には伝送路が３つであることから、本体部５０，６０は、送信データと秘匿鍵の振り分け方が本体部１０，２０とは異なる。
【００７１】
本体部５０，６０のメインＣＰＵ１では、まず送信データを伝送路３００Ａ～３００Ｃのいずれに送出するかを決める必要がある。これには、第１の実施の形態におけるデータの振り分けかたを応用することができる。例えば、送信データのファイルサイズが大きければ、送信データ用には伝送路３００Ａ（ＬＡＮケーブル）を選択するなど、各伝送路３００の伝送特性や送信データのサイズを考慮するようにしてもよいし、第１の変形例にて前述した▲１▼～▲５▼の基準を適用してもよい。
【００７２】
秘匿鍵については、この場合、（１）送信データを送出する伝送路を除き、残った２つの伝送路のいずれかに送出するか、（２）２つに分割し、各分割データを残った２つの伝送路に送出するかの２種類の伝送方法が考えられる。（１）の方法では、送信データの場合と同様に伝送路の選択を行うとよい。秘匿鍵の場合には、選択基準として最も優先順位が高いのは、秘匿性がより高い伝送路であると考えられる。（２）の方法では、例えば、単に秘匿鍵のコードを伝送路の数に分割することもできるし、所定の規則に基づいて秘匿鍵の各ビットを分配し、それぞれが単独では意味を成さないビット列に変換することもできる。このように秘匿鍵を分割して送信すると、秘匿鍵の不正入手が一層困難となる。
【００７３】
例えば、通信装置１０３が送信データＤ１を送出する場合についてみてみる。暗号化した送信データＤ１を伝送路３００Ａに送出するとすれば、秘匿鍵Ｋ１は、（１）伝送路３００Ｂまたは伝送路３００Ｃのいずれか一方に送出する（２）２つに分割し、分割データをそれぞれ伝送路３００Ｂ，　３００Ｃに送出することができる。こうした送信データと秘匿鍵の振り分けは、暗号化した送信データＤ２を伝送路３００Ｂに送出する場合、および暗号化した送信データＤ３を伝送路３００Ｃに送出する場合についても、同様に行うことができる。
【００７４】
このとき、受信側の通信装置２０３では、別々の伝送路３００から送信データＤ１と秘匿鍵Ｋ１が送られてくるが、本体部６０は、送信データＤ１と秘匿鍵Ｋ１を対として受け取り、処理すればよいので、その動作が伝送路３００の種類や数に影響されることはない。その際、秘匿鍵Ｋ１が分割データとなっていても、１つのコードに復元することにより、やはり第１の実施の形態と同様に動作することができる。
【００７５】
なお、以上は、通信装置１０３を送信側、通信装置２０３を受信側として説明したが、逆に通信装置２０３を送信側、通信装置１０３を受信側とした場合にも同様の動作を行うようになっている。
【００７６】
このように本実施の形態における通信システムは、３つの伝送路３００Ａ～３００Ｃに暗号化した送信データと暗号化に用いた秘匿鍵を振り分けて伝送するようにしたので、第１の実施の形態と同様、データ漏洩のリスク軽減の効果を奏すると共に、伝送路選択の幅が拡がったことで、その効果を高めることができる。
【００７７】
〔第４の実施の形態〕

上記の各実施の形態では、伝送路３００のそれぞれが互いに物理的に異なった伝送媒体である場合について説明した。しかしながら、本発明における伝送路は情報を互いに異なる形式で伝送するものであれば足りることから、同種の伝送媒体、もしくは同一の伝送媒体において、互いに適用する通信方式が異なるものや互いに適用する周波数帯が異なるものも、それぞれ独立した伝送経路とみなされる。本実施の形態では、そのような一例として、電力線を用いた通信システムについて説明する。

【００７８】

図１５は、本実施の形態に係る通信システムの構成を表している。ここでは、通信装置１０４と通信装置２０４とが、１つの伝送路３１０（電力線）を介して互いに送受信するようになっている。ただし、通信装置１０４は通信制御部１２Ａ，１２Ｂ、通信装置２０４は通信制御部２２Ａ，２２Ｂのそれぞれにおいて、送信データと秘匿鍵を互いに異なる周波数帯域３１０Ａ，３１０Ｂの信号に変換し、それぞれを同一の伝送路３１０に送出するようになっている。

【００７９】

図１６は、このうち通信装置１０４の構成を表したものである。なお、通信装置２０４は、対応する構成要素が同様に構成されている。本体部１０は、第１の実施の形態と同様であるが、ここでは、本体部１０は通信制御部１２Ａ，１２Ｂを介在させて伝送路３１０に接続されている。

【００８０】

通信制御部１２Ａ，１２Ｂのそれぞれは、例えば、ＡＣ用物理層機能部８Ｂの代わりにＡＣ用物理層機能部１８Ａ，１８Ｂを備えたこと以外は、第１の実施の形態における通信制御部１１Ｂと同様の構成となっている。ＡＣ用物理層機能部１８Ａ，１８Ｂは、互いに異なる周波数帯域３１０Ａ，３１０Ｂにおいて変復調を行うようになっており、その変調方式にはＦＤＭやＯＦＤＭ等が適用される。また、ＡＣ用物理層機能部１８Ａ，１８Ｂはともに伝送路３１０を媒体とするが、異なる伝送帯域を別々に利用することによって信号の送受信を互いに独立して行うようになっている。

【００８１】

次に、この通信システムの動作について説明する。図１７は、本実施の形態における通信システムの通信動作を示すフローチャートである。ここでは、一例として、暗号化した送信データＤ１とその暗号化に用いた秘匿鍵Ｋ１を、通信装置１０４から通信装置２０４に送信する場合について説明する。

【００８２】

まず、通信装置１０４の本体部１０において、送信しようとするデータＤ１を暗号化部２が暗号化することにより、秘匿鍵Ｋ１が生成される（ステップＳ２１）。次いで、送信データＤ１，秘匿鍵Ｋ１は、メインＣＰＵ１に入力され、通信制御部１２Ａ，１２Ｂに向けて振り分けられる（ステップＳ２２）。例えば、周波数帯域３１０Ａは、周波数帯域３１０Ｂよりも高周波側にあり、伝送速度も速いものとすると、送信データＤ１を周波数帯域３１０Ａに送出するように通信制御部１２Ａに出力し、それほどサイズが大きくならないことが想定される秘匿鍵Ｋ１を周波数帯域３１０Ｂに送出すべく、通信制御部１２Ｂに出力することが考えられる。

【００８３】

メインＣＰＵ１から送出された送信データＤ１は、Ｉ／Ｏ部４Ａを介して通信制御部１２Ａに入力され（ステップＳ２３）、秘匿鍵Ｋ１は、Ｉ／Ｏ部４Ｂを介して通信制御部１２Ｂに入力される（ステップＳ２６）。

【００８４】

〈変調〉

通信制御部１２Ａでは、送信データＤ１を信号に変換する。特に、ＡＣ用物理層機能部１８Ａにおいて、周波数帯域３１０Ａによる変調が施され（ステップＳ２４）、伝送路３１０に送出される（ステップＳ２５）。

【００８５】

一方、通信制御部１２Ｂでは、秘匿鍵Ｋ１が同様に信号に変換される。こちら側では、ＡＣ用物理層機能部１８Ｂにおいて、周波数帯域３１０Ｂによる変調が施され（ステップＳ２７）、伝送路３１０に送出される（ステップＳ２８）。

【００８６】

こうして、それぞれ別々に送出された送信データＤ１，秘匿鍵Ｋ１は、互いに異なる伝送帯域を利用しつつ、同一の媒体である伝送路３１０によって伝送される（ステップＳ２９）。

【００８７】

さらに、送信データＤ１は、通信装置２０４の通信制御部２２Ａに入力され（ステップＳ３０）、秘匿鍵Ｋ１は通信制御部２２Ｂに入力される（ステップＳ３２）。

【００８８】

〈復調〉

送信データＤ１は、通信制御部２２Ａにて、通信制御部１２Ａで施された過程とは逆の過程を辿ることにより、復調される（ステップＳ３１）。秘匿鍵Ｋ１も同様に、通信制御部２２Ｂにて復調される（ステップＳ３３）。

【００８９】

復調された送信データＤ１，秘匿鍵Ｋ１は本体部２０に入力され、メインＣＰＵ１を介して復号部３に入力される（ステップＳ３４）。復号部３では、秘匿鍵Ｋ１を用いて送信データＤ１が解読される（ステップＳ３５）。

【００９０】

なお、以上の動作は、通信装置２０４から通信装置１０４へデータを送信する場合であっても同様に行うことができる。また、本実施の形態では、１つの伝送路３１０を用いるようにしたが、これは、通常の電力線が２重に敷設されていないことによる。ただし、電力線が２重（またはそれ以上）に敷設されている場所においてはその限りではなく、２つ（以上）の電力線を利用し、それぞれに異なる伝送帯域を割り当てるようにしてもよい。さらに、秘匿鍵を、２つ以上の周波数帯に分割して伝送することもできる。なお、このように送信データと秘匿鍵を異なる周波数帯域を利用して伝送する例としては、電力線通信のほかに無線通信が挙げられる。

【００９１】

このように本実施の形態では、送信データと秘匿鍵を、変調帯域が異なることにより区別される経路により伝送するようにしたので、同種の伝送媒体や単一の伝送媒体においても、送信データと秘匿鍵の両方を傍受などによって不正に取得される可能性が低くなる。よって、こうした方法によっても、第１の実施の形態と同様の効果を奏することができる。

【００９２】

なお、本発明は、上記実施の形態および変形例に限定されず、種々の変形実施が可能である。例えば、上記実施の形態では、送信データは暗号化によって秘匿されるようにしたが、第３者に対し秘密にする手段であればよく、例えば暗号化以外にパスワードなどを用いて秘匿化することができる。この場合、パスワードが秘匿鍵に相応し、パスワードには、装置に割り振られたＩＰアドレスやＭＡＣアドレスを使うことができる。

【００９３】

また、上記実施の形態では、送受信を行う２つの通信装置間における伝送路は２つまたは３つとした場合について説明したが、これに限らず、３つ以上の伝送路が多重に併設されていてもよい。こうすることによって、より多くの伝送路に秘匿鍵を分割して伝送することができ、またデータ振り分けの自由度が高くなるために、データの安全性を高めることができる。

【００９４】

また、各実施の形態においては、伝送路３００，３１０で接続された２つの通信装置を双方とも送受信できるようにしたが、実際のネットワークの態様に合わせ、少なくともいずれか一方が送信機または受信機（例えばプリンタである場合など）としてのみ機能する機器としても構わない。

【００９５】
これに関連して、本発明は、通信装置の接続形態を１対１に限定するものではなく、取り得るいろいろな態様（バス型、スター型など）において適宜に適用することができる。図１８は、そうした構成の簡単な具体例を示している。通信装置１２１，１２２，１２３は、伝送路３２０Ａ，３２０Ｂによって接続されている。伝送路３２０Ａ，３２０Ｂは、ＬＡＮケーブル，電力線，　無線等どのような種類の媒体であってもよい。その接続関係は、通信装置１２１に通信装置１２２，１２３が接続された１対多対応である場合もあるし、３者が相互に接続されている場合もある。いずれにしても、伝送路３２０Ａ，３２０Ｂを利用して、送信データと秘匿鍵とを振り分けて伝送することが可能となっている。さらに、通信装置１４０のように、単一の伝送路１４１によってネットワークに接続されているために、データを振り分けて伝送することができない機器も、適宜に存在していて構わない。

【００９６】
また、こうしたネットワークを構築するにあたり、上記の各実施の形態を組み合わせて適用するようにしてもよい。なお、第２ないし第４の実施の形態に対し、第１の実施の形態における２つの変形例を適宜応用することもできる。

【００９７】
さらに、第４の実施の形態においては、変調周波数帯域が異なる場合について説明したが、そのほかにも、同種または同一の伝送媒体を用いる場合に利用できる互いに異なる信号変換方式として、互いに異なる通信方式を利用する場合が挙げられる。具体的には、ＳＳ通信方式（Ｓｐｒｅａｄ　Ｓｐｅｃｔｒｕｍ　Ｃｏｍｍｕｎｉｃａｔｕｉｏｎ：スペクトラム拡散方式）とＯＦＤＭ方式を併用することが考えられる。前者は、盗聴が難しく、機密保護に優れ、後者は伝送速度が高いという特徴がある。そこで、前者を秘匿鍵の伝送に用い、後者を送信データの伝送に用いるとよい。

【００９８】
【発明の効果】
以上説明したように、本発明の第１の観点に係る送信機によれば、秘匿鍵を用いて秘匿化した送信データを複数の伝送路のうちの１の伝送路を経由して受信機に送信すると共に、秘匿鍵を複数の伝送路のうちの他の伝送路を経由して受信機に送信するようにしたので、送信データと秘匿鍵とは互いに異なる伝送路により別々に伝送され、両方が同時に傍受されるおそれが減る。したがって、データ漏洩のリスクが軽減され、通信情報の秘密保護を強化することが可能となる。

【００９９】
また、本発明の第２の観点に係る送信機によれば、互いに異なる周波数帯の複数の搬送波を利用して受信機との間で通信を行う送信機であって、秘匿鍵を用いて秘匿化した送信データを複数の搬送波のうちの１の搬送波を用いて受信機に送信すると共に、秘匿鍵を複数の搬送波のうちの他の搬送波を用いて受信機に送信するようにしたので、送信データと秘匿鍵とが、互いに異なる周波数帯において別個独立して伝送され、両方が同時に傍受されるおそれが減る。よって、この場合も、通信情報の秘密保護を強化することが可能である。

【０１００】
本発明の第１の観点に係る受信機によれば、秘匿鍵を用いて秘匿化された送信データを、複数の伝送路のうちの１の伝送路を経由して送信機から受信すると共に、秘匿鍵を、複数の伝送路のうちの他の伝送路を経由して送信機から受信するようにしたので、本発明の第１の観点に係る送信機との間で、秘匿鍵とこの秘匿鍵を使って秘匿化した送信データとを互いに異なる伝送路に伝送する方式による通信を可能とする。

【０１０１】
なお、本発明の第２の観点に係る受信機によれば、秘匿鍵を用いて秘匿化され、複数の搬送波のうちの１の搬送波を用いて送信機から送信された送信データを受信すると共に、複数の搬送波のうちの他の搬送波を用いて送信機から送信された秘匿鍵を受信するようにし

たので、本発明の第２の観点に係る送信機との間で秘匿鍵とこの秘匿鍵を使って秘匿化した送信データとを互いに異なる伝送帯域に伝送する方式での通信を可能とする。

【０１０２】

さらに、本発明による通信システム、および本発明による通信方法によれば、送信機は、秘匿鍵を用いて秘匿化した送信データを複数の伝送路のうちの１の伝送路を経由して受信機に送信すると共に、秘匿鍵を複数の伝送路のうちの他の伝送路を経由して受信機に送信し、受信機は、秘匿鍵を用いて秘匿化された送信データを１の伝送路を経由して受信すると共に、秘匿鍵を他の伝送路を経由して受信するようにしたので、秘匿鍵とこの秘匿鍵を使って秘匿化した送信データとを互いに異なる伝送路に伝送する方式での通信を実現することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係る通信システムの構成図である。

【図２】図１に示した通信装置の構成を表すブロック図である。

【図３】図１に示した通信システムにおける基本的なデータ送受信方法を説明するための図である。

【図４】図１に示した通信システムにおける通信動作を示すフローチャートである。

【図５】図１に示した通信システムの通信動作を示すタイミングチャートである。

【図６】図１に示した通信システムにおけるデータフローブロックである。

【図７】図１に示した通信システムの第１の変形例におけるシステム構成を表す図である。

【図８】図７に示した通信システムの通信動作を示すタイミングチャートである。

【図９】図７に示した通信システムにおけるデータフローブロックである。

【図１０】図１に示した通信システムの第２の変形例におけるシステム構成を表す図である。

【図１１】図１０に示した通信装置の構成を表すブロック図図である。

【図１２】第２の実施の形態に係る通信システムの構成図である。

【図１３】図１２に示した無線用の通信制御部の構成を表すブロック図である。

【図１４】第３の実施の形態に係る通信システムの構成図である。

【図１５】第４の実施の形態に係る通信システムの構成図である。

【図１６】図１５に示した通信装置の構成を表すブロック図である。

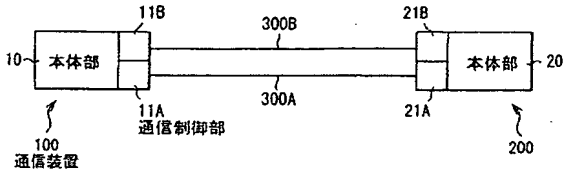
【図１７】図１５に示した通信システムの通信動作を示すフローチャートである。

【図１８】本発明の通信システムの一具体例を表す図である。

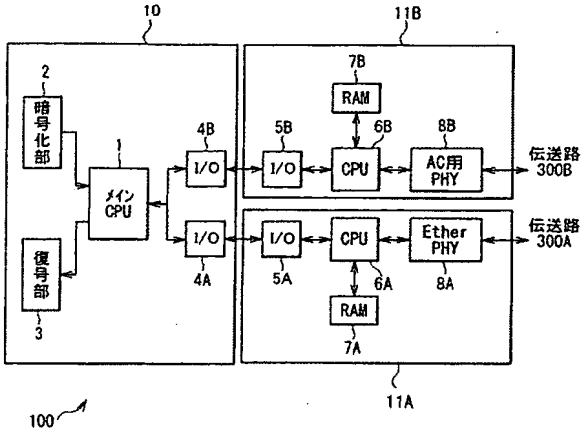
【符号の説明】

１…メインＣＰＵ、２…暗号化部、３…復号部、４Ａ，４Ｂ…Ｉ／Ｏ部（本体部側）５，５Ａ～５Ｃ…Ｉ／Ｏ部（通信制御部側）、６Ａ～６Ｃ…ＣＰＵ、７Ａ～７Ｃ…ＲＡＭ、８Ａ…イーサネット（Ｒ）物理層機能部、８Ｂ，１８Ａ，１８Ｂ…ＡＣ用物理層機能部、８Ｃ…無線用物理層機能部、１０，２０，３０，４０，５０，６０…本体部、１１，１１Ａ～１１Ｃ，１２Ａ，１２Ｂ，２１，２１Ａ～２１Ｃ，２２Ａ，２２Ｂ…通信制御部、１００～１０４，１２１～１２３，２００～２０４…通信装置、３００，３００Ａ～３００Ｃ，３１０，３２０Ａ，３２０Ｂ…伝送路、３１０Ａ，３１０Ｂ…周波数帯域、Ｄ１，Ｄ２…送信データ、Ｋ１，Ｋ２…秘匿鍵

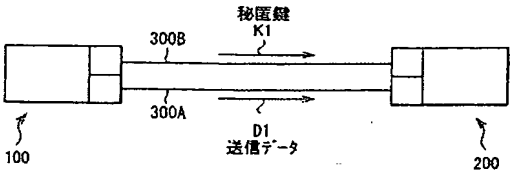
【図1】



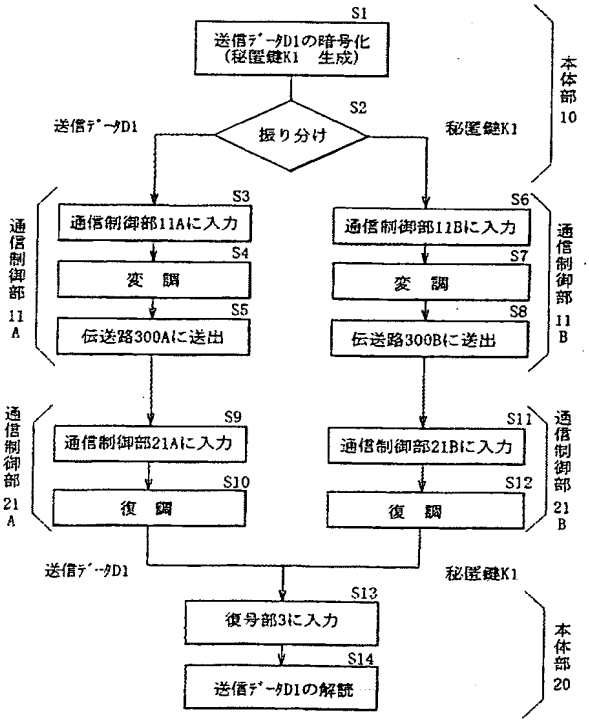
【図2】



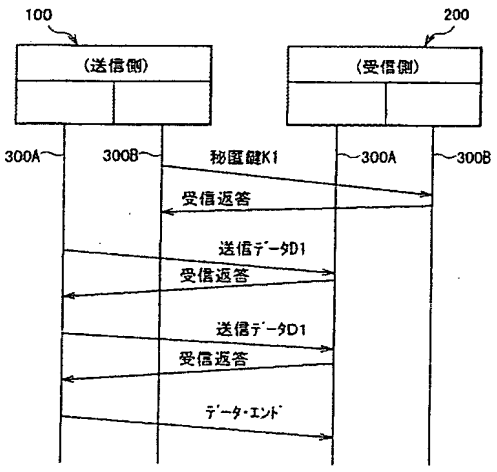
【図3】



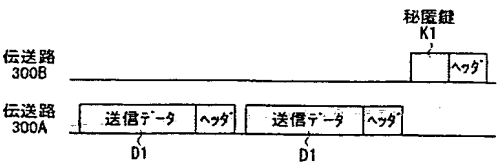
【図4】



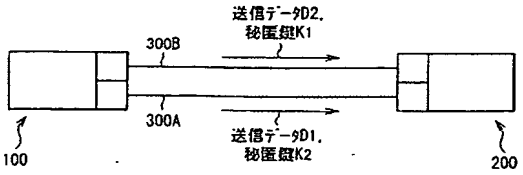
【図5】



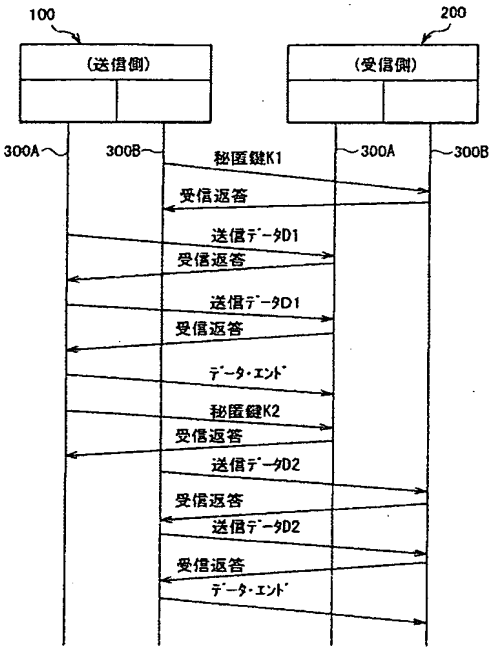
【図6】



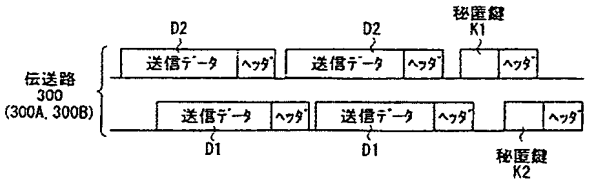
【図7】



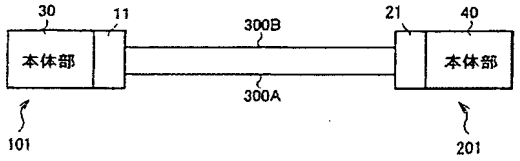
【図8】



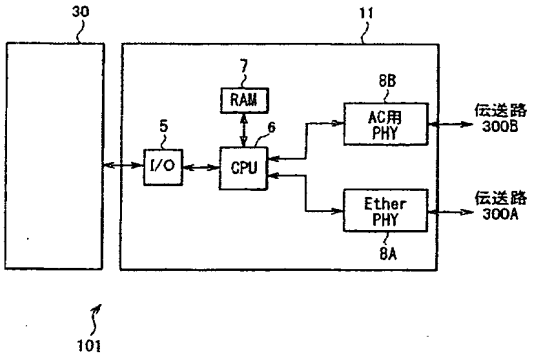
【図9】



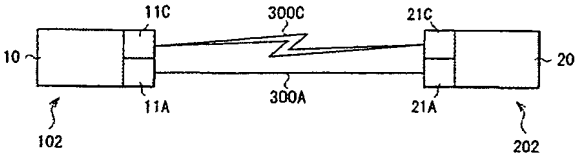
【図10】



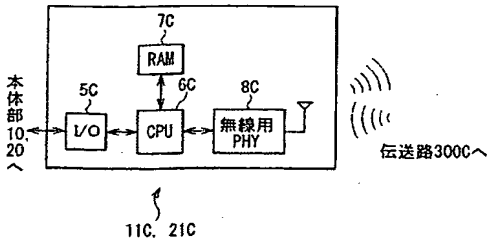
【図11】



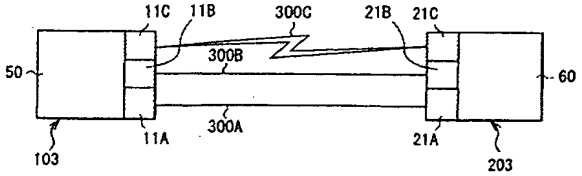
【図12】



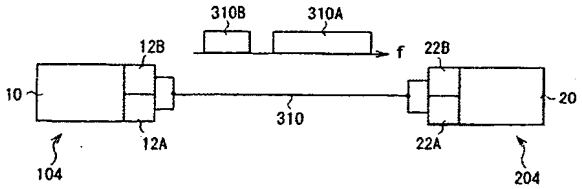
【図13】



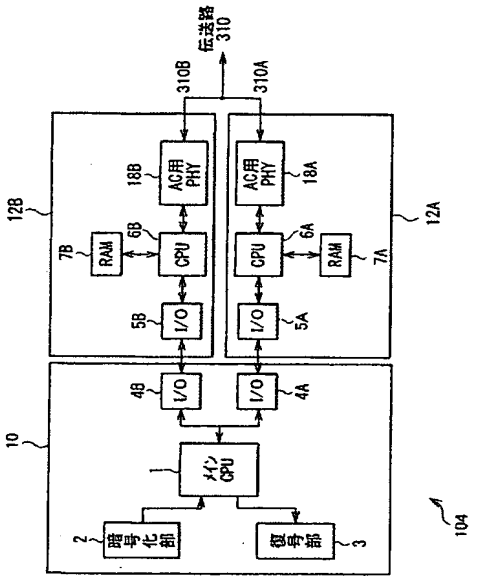
【図14】



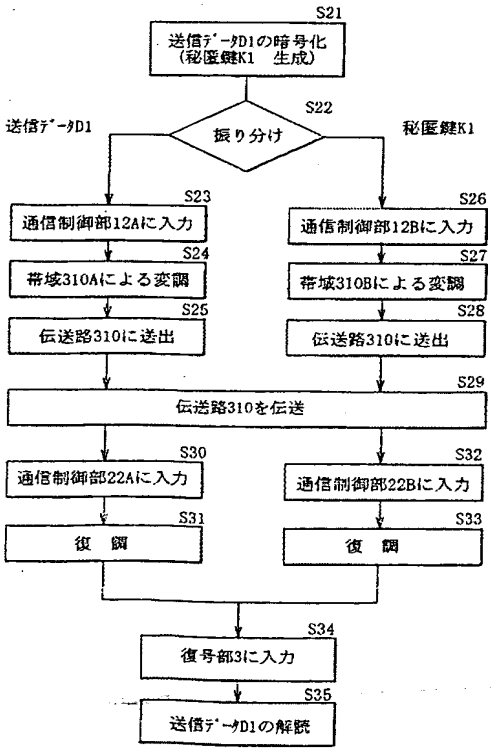
【図15】



【図16】



【図17】



【図18】